PENETRATION TESTING AND VULNERABILITY ANALYSIS SYLLABUS

Module 1: Pentesting Fundamentals

- Vulnerability Assessment (VA) vs. Pentesting Analysis (PTA)
- Types of Vulnerability Assessments
- Modern Vulnerability Management Program
- Ethical Hacking Terminology
- Five Stages of Hacking
- Vulnerability Research
- Impact of Hacking
- Legal Implications of Hacking
- Comparison of VA and PT Tools

Module 2: Information Gathering Methodologies

- Competitive Intelligence
- DNS Enumeration
- Social Engineering Attacks
- Scanning and Enumeration
- Port Scanning:
    - Network Scanning
    - Vulnerability Scanning
    - Scanning Tools
- OS and Fingerprinting Enumeration
- System Hacking Passwords

Module 3: System Hacking

- Password Cracking Techniques
- Key Loggers
- Escalating Privileges
- Hiding Files
- Active and Passive Sniffing
- ARP Poisoning
- IP Poisoning and MAC Flooding

Module 4: Wireless Pentesting

- Wi-Fi Authentication Modes
- Bypassing WLAN Authentication
- Types of Wireless Encryption
- WLAN Encryption Flaws
- Access Point Attacks
- Attacks on the WLAN Infrastructure
- Buffer Overloading

Module 5: The Metasploit Framework

- Metasploit User Interfaces and Setup
- Getting Familiar with MSF Syntax
- Database Access
- Auxiliary Modules
- Payloads:
    - Staged vs Non-Staged Payloads
    - Meterpreter Payloads
- Experimenting with Meterpreter

Module 6: Web Application Attacks

- Web Application Assessment Methodology
- Enumeration
- Inspecting URLs
- Inspecting Page Content
- Viewing Response Headers
- Inspecting Sitemaps
- Locating Administration Consoles

Module 7: Exploiting Web-Based Vulnerabilities

- Exploiting Admin Consoles
- Cross-Site Scripting (XSS)
- SQL Injection